



SECURING DIGITAL EVIDENCE: BLOCKCHAIN AND AES-ENCRYPTION FOR TAMPER-RESISTANT DATA INTEGRITY IN CYBERCRIME INVESTIGATIONS

Dr. P. Maragathavalli¹, Aravindhar RS², Keerthana R.³, Harini M.⁴, Sanjay Kumar S.⁵

^{1, 2, 3, 4, 5} Puducherry Technological University, Puducherry

ABSTRACT

Cybercrime gives challenges to law enforcement agencies to secure digital evidence and maintain its integrity. Blockchain known for its decentralized and immutable nature, provides a secure ledger to record digital evidence transactions restricting unauthorized access. This project proposes a framework for digital forensic evidence management, contributing to the enhancement of security and reliability in digital forensic practices through the utilization of Ethereum Blockchain technology and Advanced Encryption Standard (AES) encryption. Through a systematic review, various studies, methodologies, and implementations employing Blockchain to safeguard digital evidence are explored. Blockchain, known for its decentralized and immutable nature, provides a secure ledger to record digital evidence transactions, restricting unauthorized access. Advanced Encryption Standard (AES) algorithm ensures that the data stored on the blockchain remains tamper-resistant and secure. In the blockchain ecosystem, Proof of Stake (POS) plays a critical role by facilitating transaction validation and block creation. It distinguishes itself by selecting validators based on the amount of cryptocurrency they 'stake' or pledge as collateral, offering an energy-efficient and environmentally sustainable alternative to the traditional method.

KEYWORDS: Cybercrime, Blockchain, Tamper-Resistant, Decentralization, Data Integrity, Digital Forensics, Advanced Encryption Standard (AES), Proof of Stake (PoS)

INTRODUCTION

In today's ever-evolving digital landscape, the proliferation of technology has brought about unprecedented challenges in securing our digital infrastructures against a multitude of cybersecurity incidents. As our world becomes increasingly interconnected, the importance of digital forensics has grown exponentially, making it an essential tool in investigating and mitigating the impact of cybercrimes. The rapid advancement of technology and the growing sophistication of cybercriminals have made it imperative to leverage digital forensics to its fullest potential.

This field encompasses a comprehensive set of methodologies and techniques that are used to collect, store, analyse, and present critical evidence necessary for convicting individuals involved in cybercrimes. These investigations delve into the acquisition, analysis, detailed evaluation, and interpretation of the digital evidence associated with the incident, providing invaluable insights into the incident's origins, motives, and methodologies employed.

Maintaining the integrity and accuracy of forensic evidence is of paramount importance in the field of digital forensics. Any compromise in the handling or preservation of evidence can lead to its inadmissibility in court, potentially jeopardizing the pursuit of justice. To address this concern, meticulous procedures are employed, collectively known as the "chain of custody." "The chain of custody (CoC) is a documented trail that meticulously tracks the handling of evidence from the moment it is collected at the crime scene or from digital systems until it

is presented in a court of law.

This trail ensures that the evidence is handled, stored, and transferred in a manner that preserves its integrity and authenticity. The chain of custody is not only crucial for the credibility of digital evidence but also for upholding the principles of fairness and due process in legal proceedings.

In light of the growing importance of digital forensics and the critical role it plays in cybersecurity, it is essential to explore innovative approaches to enhance its effectiveness. This project proposes the use of advanced prediction algorithms, namely Proof of Stake (PoS) and Advanced Encryption Standard (AES), to augment the capabilities of digital forensics. By integrating these cutting-edge technologies, we aim to elevate the field of digital forensics, making it more agile, efficient, and adaptable in the face of evolving cyber threats.

Blockchain Technology

Blockchain technology is a revolutionary innovation that has transformed the way we think about data management and trust in the digital age. At its core, blockchain is a decentralized and distributed ledger system that ensures transparency, security, and immutability of recorded transactions. This technology has transcended its origins in cryptocurrencies to find applications across various industries, from supply chain management and healthcare to finance and beyond.

By eliminating the need for intermediaries and providing a tamper-resistant ledger, blockchain has the potential to

streamline processes, reduce fraud, and enhance trust in transactions. Its decentralized nature, cryptographic security, and smart contract capabilities make it a powerful tool for creating a more efficient and trustworthy digital ecosystem. As blockchain continues to evolve and mature, its impact on industries and society as a whole is poised to grow, ushering in a new era of transparency and innovation.

Advanced Encryption Standard

The Advanced Encryption Standard (AES) stands as a pinnacle of modern cryptographic security. It is a symmetric encryption algorithm celebrated for its strength and efficiency, capable of safeguarding sensitive data across a plethora of applications. AES operates by dividing data into fixed-size blocks and applies a series of complex mathematical operations in multiple rounds. Key expansion further enhances security by generating round keys from an original encryption key.

AES supports various key lengths, with longer keys providing stronger protection against cryptographic attacks. With its resistance to brute force attacks and its wide adoption in secure communication, file encryption, and more, AES is a global standard trusted to protect data privacy and security in an increasingly digital world.

Proof Of Stake

Proof of Stake (PoS) is a blockchain consensus mechanism that distinguishes itself from the energy-intensive Proof of Work (PoW). In PoS, validators are chosen to create blocks and confirm transactions based on the cryptocurrency coins they hold and are willing to “stake” as collateral. This approach not only drastically reduces energy consumption but also incentivizes validators to act honestly to safeguard their staked assets, enhancing security. PoS offers scalability advantages, enabling more inclusive participation models and achieving faster transaction finality. While it has security benefits, it also introduces considerations related to centralization risks. PoS, and its variant Delegated Proof of Stake (DPoS), are influential in shaping the future of blockchain networks due to their efficiency and sustainability.

MATERIALS AND METHODS

In this section, we use these 4 technologies to implement our project

A. Advanced Encryption Standard:

The Advanced Encryption Standard (AES) is a widely used encryption algorithm that ensures data confidentiality and integrity. It employs symmetric key encryption, where the same key is used for both encryption and decryption. AES is known for its security, efficiency, and speed, making it ideal for securing sensitive information in various applications, including blockchain technology.

B. Ethereum Blockchain:

Ethereum blockchain is a decentralized platform that enables the creation and execution of smart contracts and decentralized applications (DApps). It operates as a distributed ledger, recording transactions across a network of computers, known

as nodes. Ethereum’s native cryptocurrency, Ether (ETH), is used as fuel for executing smart contracts and transactions on the network. One of Ethereum’s key features is its ability to support the development of DApps through its Turing-complete programming language, Solidity. This flexibility has led to a wide range of use cases, including decentralized finance (DeFi), non-fungible tokens (NFTs), and various other applications beyond simple financial transactions.

C. IPFS:

IPFS (InterPlanetary File System) is a decentralized protocol and network for storing and sharing content on the internet. It uses unique content addressing, decentralized distribution, and caching to enable efficient and secure retrieval of files without relying on centralized servers. This technology is often used in conjunction with blockchain for creating decentralized applications and services.

D. Proof Of Stake:

Proof of Stake (PoS) is a consensus algorithm used in blockchain networks to validate transactions and create new blocks. In PoS, validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to “stake” or lock up as collateral. This system aims to achieve consensus and secure the network in a more energy-efficient and environmentally friendly manner compared to Proof of Work (PoW) algorithms. Validators are incentivized to act honestly since their staked coins are at risk of being forfeited if they attempt to validate fraudulent transactions. PoS is known for its scalability and reduced energy consumption, making it an attractive alternative to PoW for many blockchain projects.

Project Workflow

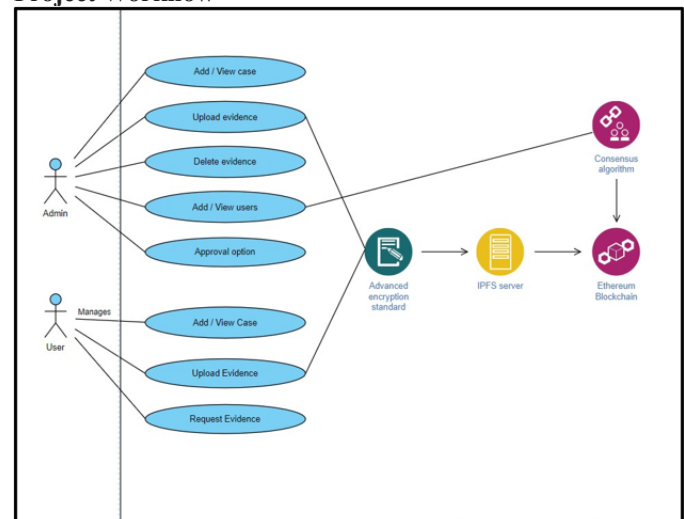


Figure 1: Proposed system

The project (Fig 1) flow begins with the admin logging in, granting them full control over system activities, including managing users, approving registrations, and viewing evidence. Users can register, awaiting approval from the admin. Upon approval, users gain access to adding and viewing evidence in the system. When storing data, it undergoes AES encryption before being stored on IPFS, ensuring its confidentiality and integrity. Transaction details are recorded on the blockchain for

transparency and traceability. To view encrypted evidence, the user requests the key from the admin, providing an additional layer of security. This seamless flow ensures that only approved users can interact with the system, with data stored securely and access tightly controlled, making it a robust solution for digital forensic evidence management.

Admin Module

I. Evidence Management:

View Evidence: The Control Room has the authority to view and delete evidence files uploaded by users from various police stations for specific case IDs. Each evidence file is assigned a unique code ID generated by IPFS (Fig 3) for identification and retrieval purposes.

Upload Evidence: The Control Room can add evidence files for any respective case ID, irrespective of the format or size of the files (text, images, videos).

II. User Management:

View Users: The Control Room has the capability to view and delete users who have uploaded evidence files across different police stations. Additionally, the Control Room can access the address and key value associated with each user's account on the Ethereum blockchain (Ganache) (Fig 4), providing a transparent record of user activities.

Access Rights Management: The Control Room has the authority to grant access rights to users, allowing them to view evidence files uploaded by other users across various police stations. This feature facilitates collaboration and information sharing among law enforcement personnel.

III. Case Management:

View Cases: The Control Room can access and monitor ongoing cases across the city, providing a centralized overview of law enforcement activities and resource allocation.

User Module

I. Case Filing

Upload Evidence: Police stations have the authority to add evidence files collected during investigations for any respective case ID. This includes text, images, and videos in various formats and sizes, ensuring comprehensive documentation of case details and evidence.


II. Evidence Management:

View Evidence: Police stations can view and delete evidence files associated with specific case IDs. Each evidence file is assigned a unique code ID generated by IPFS, facilitating easy identification and retrieval of evidence during case proceedings.

Access Evidence: Upon approval by the admin, police stations can access evidence files submitted by other users for a particular case. This feature enhances collaboration and information sharing among law enforcement agencies, leading to more effective case resolution.

RESULTS AND DISCUSSION

Screenshots



did	filename	codeid	caseid	actions
1	QUIZ2.jpg	QmawUQ9hwhfHgeK5SeYVScFicDwUddgBhQoqlyYb04	c1	Details Download
2	File_example_MP4_480_1_SMG.mp4	QmeibohuG2pM1t9b67J25eU7c0AAAbdyT7u3aPhmZj	c1	Details Download

Figure 2: Uploaded Evidences

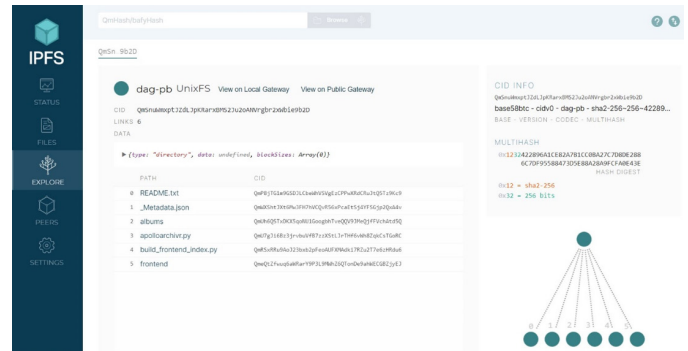
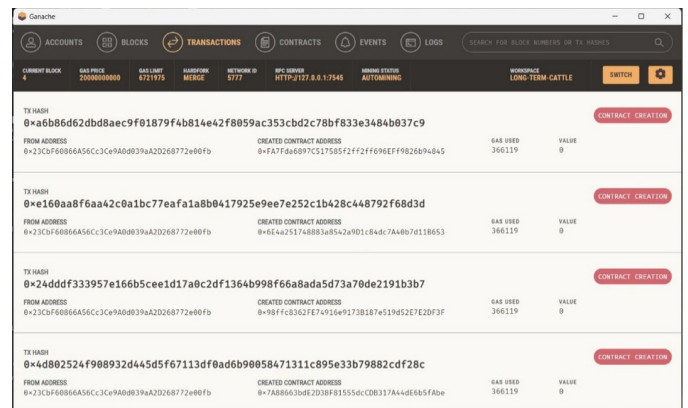


Figure 3: Evidence in IPFS



TX HASH	FROM ADDRESS	CREATED CONTRACT ADDRESS	GAS USED	VALUE
0xa6b86d62dbd8aec9f81879fb814e42f8059ac353bd2c78bf833e3484b637c9	0x23Cf68866A56C3C9A080839A20268772e0f0	0x7A7F6A6897C517585F2F2F696EF982694B45	366119	0
0xe160aa8f6aa42c8a1bc77ea1a8b0417925e9ee7e252c1b428c44872f68d3d	0x23Cf68866A56C3C9A080839A20268772e0f0	0x6Caa251748883a5a2a9D1c84dc7Aa8b7d118653	366119	0
0x24dddf33395f1e6b5ccee1d17a0c2df1364b998f66a8ada5d73a70de2191b3b7	0x23Cf68866A56C3C9A080839A20268772e0f0	0x98FFC8362F7E74916a917381874519452E7E20F3F	366119	0
0x4d802524f988932d445d5f6113df8ad6b9085847131c895e33b79882cdf28c	0x23Cf68866A56C3C9A080839A20268772e0f0	0x7A88630d12038F8155dcDB317Aa4d6b5FA0e	366119	0

Figure 4: Users registered in blockchain

By integrating Ethereum blockchain with AES encryption and IPFS storage, our project “Securing Digital Forensic Evidences in Blockchain Using AES” achieves a robust level of security. Through smart contracts, users are securely created, while their data undergoes encryption using AES before being stored on the IPFS server with corresponding hash values recorded on the blockchain and in the database. This multilayered approach ensures tamper-proof evidence storage. Moreover, granting exclusive access to the admin for monitoring all system logs and transactions adds an extra layer of security. Users must request access from the admin to view any evidence, enhancing control over data access. This comprehensive system design not only provides data integrity and confidentiality through blockchain and AES but also ensures strict oversight and controlled access, making it a highly secure solution for digital forensic evidence management.

CONCLUSION

While blockchain technology holds significant promise for enhancing chain of evidence management, several challenges must be addressed to realize its full potential. Issues such as slow transaction speeds in cold blockchains, system

complexity, security vulnerabilities during data transmission, and interoperability concerns require focused attention. By addressing these challenges, the field can move towards creating more efficient, secure, and user-friendly solutions that meet the demands of law enforcement operations and legal proceedings, ultimately improving the integrity of the chain of evidence. Integration of AES encryption and Solidity smart contracts in our project represents a commendable step towards bolstering the security of digital evidence within blockchain systems for cybercrime investigations. Recognizing the current limitation of unencrypted data storage in the blockchain, the application of AES encryption protects unauthorized access and tampering. As a future consideration, continued exploration of cutting-edge encryption technologies and key management strategies will be essential to stay ahead of evolving cybersecurity.

REFERENCES

1. Charan, T. S., & Sowmyashree, K. M. (2022). Criminal Digital Forensic Investigation Application based on Blockchain. *International Research Journal of Engineering and Technology (IRJET)*, 08(06), e-ISSN: 2395-0056, p.196-200.
2. Elgohary, H. M., Darwish, S. M., & Elkaffas, S. M. (2022). Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications. *IEEE Access*, 10, DOI: 10.1109/ACCESS.2022.3147809, p. 14669-14679.
3. Khan, A. A., Uddin, M., Shaikh, A. A., Laghari, A. A., & Rajput, A. E. (2021). Ledger: Blockchain Hyperledger Sawtooth Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture. *IEEE Access*, 9, DOI: 10.1109/ACCESS.2021.3099037, p.103637-103650.
4. Kim, D., Ihm, S.-Y., & Son, Y. (2021). Two-Level Blockchain System for Digital Crime Evidence Management. *MDPI AG (Multidisciplinary Digital Publishing Institute) Sensors*, 21(3051), 1-17. DOI: 10.3390/s210930, p.1-17
5. Lone, A. H., & Mir, R. N. (2017). Forensic-Chain: Ethereum Blockchain Based Digital Forensics Chain of Custody. *Scientific and Practical Cyber Security Journal (SPCSJ)*, 1(2), 21-27, Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667, p. 21-27
6. Prakash, F., & Sadawarti, H. (2023). A Blockchain-Based Chain of Custody for Digital Forensic Investigations. *European Chemical Bulletin*, 5, ISSN 2063-5346, p.3187-3193.
7. Renuka, B., & Kusuma, S. (2021). Blockchain based Digital Forensics Investigation Framework. *International Research Journal of Engineering and Technology (IRJET)*, 08(06), 4073-4077. eISSN: 2395-0056, p.4073 -4077.
8. Shetty, S., Shinde, K., Shelke, D., Garje, R., & Mahtre, A. (2023). Crime Evidence Over Blockchain. *International Journal of Scientific Research in Engineering and Management (IJSREM)*, 07(042022), DOI: 10.55041/IJSREM18619, ISSN: 2582-3930, p. 1-4.
9. Shrunga, H. S., Ashwini, M., Deepthi, U., Spandana, R., & Rakesh, K. R. (2022). A Survey on Blockchain Based Digital Forensics Framework. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 10(IV), 2542-2549. ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538, p. 2542 - 2549.
10. Ziar, R. A et al. (2021). Privacy Preservation for On-Chain Data in the Permissionless Blockchain using Symmetric Key Encryption and Smart Contract. *Mehran University Research Journal of Engineering and Technology*, 40(2), 305-313. DOI: 10.22581/muet1982.2102.05, p. 305-313.